500TH MI BRIGADE
CRITICAL INFORMATION GUIDE

This Critical Information Guide identifies 500th MI Brigade's Critical Information or Essential Elements of Friendly Information (EEFI) that requires our protection.

I. Personnel/Position Strength

- Work schedules, operations and personnel actions that indicate changes in OPTEMPO
- Unit identifiers with deployment/re-deployment dates
- Personnel information listing duties, names, ranks and positions
- Personal info of personnel assigned to the 500th MI Brigade or subordinate units requiring protection IAW FOIA & the Privacy Act.

II. Intelligence

- 500th MI Brigade intelligence & collection capabilities, requirements, limitations and priorities
- Requests for information or equipment
- US counterintelligence investigative and intelligence collection capabilities, requirements and priorities

III. Operations

- Mission signature and profiles
- Actions before, during or after preparing for missions or deployments
- Response planning and execution results
- 500th MI Brigade, Order of Battle information
- Location, itineraries, and travel modes of key leadership and Distinguished Visitors
- Force Protection operations
- Information pertaining to staff duty officer and guard duties which could risk lives of participating personnel
- Weapon storage and security capabilities
- Target or collection lists, rules of engagement and any other constraints placed on operations
- After Action Reports (AAR) or Exercise Summaries (EXSUM) conveying friendly information and weaknesses
- Inspection results revealing vulnerabilities to espionage, sabotage, penetration or terrorist attack
- Changes in THREATCON and INFOCON implementation measures

IV. Logistics

- Major supply points, re-supply items & schedules -- shortfalls, & special storage
- Info on sole source suppliers and providers of 500th MI Brigade critical items
- Info on commercial support contracts
- Sequence of logistical events and transportation schedules.
- Identity and location of munitions by type, quantity, and destructive capability
- Receipt, installation of special equipment
- Storage locations, procedures, and processes for storage of unit supplies/re-supply

V. Allied Nations/Alliances

- Info concerning the establishment or disestablishment of ties with any nation for purposes of military operations
- Info on any political agreements or disagreements between the U.S. and any allied nation or alliance

VI. Communications

- Communications involved in operations or support of the operation (types of comms and infrastructure, freqs, call signs, computer passwords, internet protocol (IP) addresses)
- Capabilities/limitations/vulnerabilities of communications systems
- Critical comms (links or nodes) locations or functions

VII. Force Protection

- Force protection measures and shortfalls
- Vulnerabilities of buildings and locations that could aid in espionage, sabotage, penetration or terrorist attack
- Power production and public works shortfalls (basing issues - power and water)

500TH MILITARY INTELLIGENCE BRIGADE

OPSEC

OPERATIONS SECURITY

DO YOU KNOW OPSEC ?

OPSEC provides for protection of information vital element used to protect our unit, service members and families. It is our best interest and intent to ensure that every mission conducted by 500th MI Brigade service members and civilians will deny our adversaries access to any useful information. At no time can we lower our security awareness or standards on duty or off duty. Diligence in OPSEC is key to ensuring effectiveness in the 500th MI Brigade operations and our collective safety.

SSO/S2, 500th MI Brigade – 655-1224

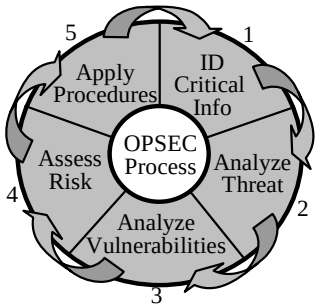
Few of us really know OPSEC!

WHAT IS OPSEC?

OPSEC is more than gates, guns, surveillance cameras and security guards. It is not a security function; it is an operational function.

Protecting critical information, both unclassified and classified from our adversaries. Through our everyday missions each of you will acquire information. Even though much of this information may be unclassified by itself, when pieced together by our adversaries, it can easily paint a picture of our mission capabilities, intentions, and weaknesses. If we are not thorough in our OPSEC procedures, an adversary may use this information against us for sabotage, espionage, subversion, or terrorism.

The OPSEC Process is a five step, interactive process designed by the Interagency OPSEC Support Staff (IOSS) and implemented by DOD to



protect our critical information from our adversaries. The five steps in the process are:

1. CRITICAL INFORMATION

See Critical Information Guide on the reverse. *Again, critical information can be classified or unclassified information!*

2. ANALYZE THE THREAT

Are our adversaries collecting on us? The answer is not an emphatic, "*Yes, most Definitely!*" The OPSEC threat *begins with you, where you are encouraged to employ security measures. Your* OPSEC Officer can assist you or you may visit the IOSS Website for more information; www.ioss.gov.

3. ANALYZE VULNERABILITY

OPSEC Indicators are friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive critical information.

OPSEC Vulnerabilities exist when an adversary can collect upon our indicators.

4. ASSESS THE RISK

What is the risk? Only when you ID your critical information, understand the threat and ID potential vulnerabilities can you gauge the risk. Ultimately the commander must approve the accepted level of risk.

5. OPSEC PROCEDURES

Anything that protects critical information or the indicators of such information is an OPSEC procedure. OPSEC procedures include: proper communications security (COMSEC) procedures; trash disposal procedures; using For Official Use Only (FOUO) caveats for personal/personnel information requiring protection under the Freedom of Information Act; applying the sensitive information (SINFO) caveat to protect unclassified information considered as critical and use appropriate classification markings to protect critical information that requires limited access.

OPSEC TIPS

Limit Web Info: In essence, anything you post on the web might as well be faxed directly to every adversary in the world!

Limit non-secure Phone & Cell Phone use: Do not discuss or talk around classified or unclassified critical information.

OPSEC IS A FAMILY AFFAIR

When 500th MI Brigade missions require us to go TDY from our home, that is an OPSEC indicator. All family members are part of the OPSEC team and need to protect group information to ensure our safety.

Discuss OPSEC with your family!

SPECIAL SECURITY OFFICER (SSO)
Information Security Operations
500th MI Brigade, Stop 202, A-Quad
Schofield Barracks, Hawaii 96857-5300
ATTN: IAPD-SE (SSO/S2)
DSN (312) 455-1224; COMM (808) 655-1224/9607